

*System i family keeps your business up and running*



**IBM System i Family —  
Resilient and Secure by Design**



## Highlights

- *Integrated system: hardware, security, system management, middleware*
- *Object-based architecture for superior resiliency characteristics*
- *Proven i5/OS® operating system with V5R4 enhancements for security*
- *High Availability and Disaster Recovery offerings*
- *Built on proven technology and backed by world-class service and support*

### **Flexible. Adaptive. Responsive. Assured.**

These are necessary attributes for businesses today. Gone is the luxury of experience and react. To compete in today's on demand world, enterprises of all sizes must be able to anticipate and adjust, sense and respond. These capabilities don't just happen. They are created through a focused and holistic approach. Once achieved, a business is said to be resilient. But what is business resiliency and why does it matter? Business resiliency is the ability to rapidly adapt and respond to opportunities, regulations and risks in order to maintain secure, continuous business operations, be a more trusted enterprise and enable your business to grow. As such, business resiliency has become an imperative. Critical to business

resiliency is the nature and character of the IT infrastructure—availability, recovery, security and compliance must be addressed. The IBM System i™ family delivers these capabilities enterprises need to achieve business resiliency.

### **Resiliency in a box**

The System i family featuring IBM i5/OS V5R4 offers state of the art availability and reliability, integrating security and virus resistance by design. These features make it easy to help secure and to maintain the security of the system. The security and business resiliency provided by i5/OS is substantiated by virus lists such as those at <http://www.sarc.com> and <http://viruslist.com> indicating that the industry has identified fewer threats to

i5/OS than to Windows® or UNIX® operating systems. High availability options such as clustering and cross-site mirroring make i5/OS environments among the most resilient in the industry. System i and i5/OS are designed for businesses that need high protection and availability for key applications and data. They help ensure operations continue after an outage or disaster, comply with government regulations and industry standards, and provide protection costs that are predictable and manageable. System i solutions help provide a solid foundation for business resiliency.

### Getting started

Business Resiliency is dependent upon risk management and information security. That makes corporate policy the proper starting point for any discussion on business resiliency. Corporate policy addresses the broad issues central to business existence and operations. In turn, the business resiliency policy derives from corporate policy, and focuses on protecting and preparing the enterprise. The IT resiliency policy derives from the business resiliency policy and applies from the network layer down to the individual systems. At the system level, the policy becomes a

specific set of requirements which will dictate your availability and security implementation.

### Essential IT responsibilities

Asset protection

- Provide for availability and recoverability of applications and data
- Ensure security of applications and data
- Provide for application change management





## Compliance

- Establish an IT policy that supports the corporate policy
- Implement and document the policy
- Test to demonstrate conformity to the documented policy

## Asset protection

### Availability management

Availability management begins with agreement inside an organization on application availability level. Availability management implementation approaches focus on single system requirements or multiple system requirements. In a single system environment, the focus is primarily backup recovery and disk protection. The implementation will depend on the

backup recovery solution and disk protection scheme that best addresses your requirements. For environments often referred to as mission critical, where the demands are for applications to be continuously available, multiple system solution environments (clustering) are deployed. In this state of the art cluster environment, impact on application availability from planned or unplanned outages must be absolutely minimal.

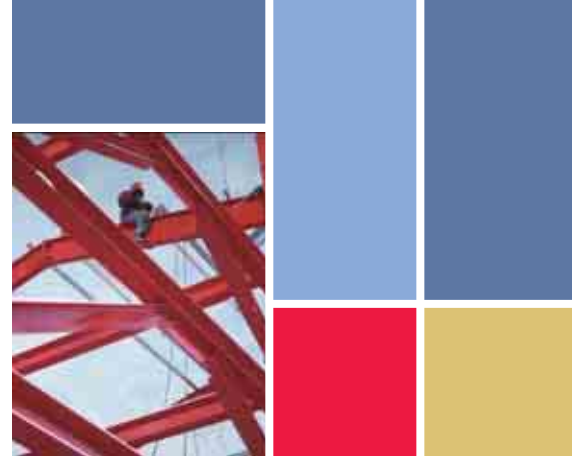
### Security management

Security of applications and data is achieved through policy creation, policy implementation and platform technologies.

### *Policy creation and implementation*

Security implementation derives from the security policy. When an audit occurs, the auditors will focus on your ability to demonstrate your compliance to your policy. A clearly articulated security policy and corresponding implementation must be the focus to enable an audit-ready posture. One approach to developing a system level security policy is to utilize a security policy development solution from System i ISVs, whose offerings harness the power of the System i capabilities of integrity protection, network intrusion detection and enhanced auditing functions.





### *Platform technologies*

All System i models are architected and designed to meet stringent security requirements. While most servers can be made secure, the System i family is designed to be easy to secure and provides easy to manage security. The System i is highly secure by design—from inception its architecture was object-based. Object-based architecture necessitates precise rules for interaction between objects. These rules translate into world-class security properties. Objects have access interfaces and rules that are unique for each object type. With proper security implementation, one object type can not masquerade as another, and only authorized objects can access one another. This means that the System i architecture does implicitly what may need to be done overtly and explicitly in other system environments. By focusing

on object level security, the System i family can enable a security policy that starts on the inside, at the most fundamental level of information management.

### **Application change management**

Application change management is about documented processes and procedures that define who may change an application and how it may be moved from a test environment into a production environment. Change management is both to ensure quality control and security. There are industry standard change management policies as well as tools to help enforce the change management process. Digital Certificates are a means of helping ensure that only authorized owners of code have changed the code and that the current level of production code has not been changed by anyone other than the authorized owner.

### **Compliance**

Compliance is the ability of your firm to demonstrate conformity to government regulations and industry standards—including those regarding information integrity. These regulations and standards evolve constantly. Their relationship to corporate requirements, internal business controls, auditing procedures and audit evidence are complex. Using the relevant regulations and standards as guides, you can create your policy. Another approach is to utilize the solutions and expertise from System i ISVs, whose offerings take advantage of the rich capabilities of the System i platform. The System i family helps you assure that your business and its technology infrastructure are meeting these critical compliance needs.



## **System i offerings for Business**

### **Resiliency**

#### **High Availability**

Are your applications available when your customers, partners and employees are ready to conduct business? High availability is the ability of your enterprise to minimize downtime, maximize up-time and generally to provide a high level of service to those who need it. System i High Availability Edition for models 520, 550, 570 and 595 provides a cost-effective approach to acquire a secondary system to help deliver on service level commitments and help meet customer expectations for 24x7 availability.

### **Disaster Recovery**

Recovery refers to your ability to return operations to business-as-usual following a catastrophic event. By creating a disaster recovery environment, you create a solution that is resilient to acts of destruction. In the case of a major catastrophic event, such as earthquake, hurricane, flood or fire, replication of centralized data to a remote location helps to ensure that operations can be resumed and critical data is safeguarded. These types of events happen only rarely—but when they do, they have the potential to destroy and can

shut down your business. The System i Capacity BackUp Edition for models 570 and 595 delivers cost effective, standby computing power available if disaster strikes.

### **Security & Compliance**

Artful and intelligent integration of hardware, security, systems management and middleware into a robust platform for business computing is the hallmark of the System i platform. i5/OS V5R4 extends the reach of System i integration to reflect the expansive nature of the on demand business world. V5R4 reinforces the proven ability of i5/OS to help safeguard data, help shield assets from hackers and help keep business



applications and data available. V5R4 security and resiliency enhancements include:

- Hardware storage protection to help prevent “rogue” programs from accessing system objects
- Intrusion detection features that administrators can use to easily automate monitoring for intrusion events, such as scanning for open TCP/IP ports
- New auditing features to strengthen access control
- Additional encryption capabilities to safeguard critical data
- Clustering enhancements that simplify management of highly-available environments
- Dual parity support (RAID-6) in a disk array for ongoing operation even if two units in a protected set of disks fail
- Automated journaling of additional system objects
- Concurrent firmware and non-disruptive fixes
- New backup options, including virtual tape support, that help enable continuous operations



## For more information

Contact your IBM representative or  
IBM Business Partner or visit:  
**ibm.com/system/i/resiliency**



© Copyright IBM Corporation 2006

IBM Corporation  
Integrated Marketing Communications  
Systems & Technology Group  
Route 100  
Somers, NY 10589

Published in the United States of America  
May 2006  
All Rights Reserved

IBM, the IBM logo, AS/400, DB2, Infoprint,  
System i and i5/OS are trademarks or registered  
trademarks of International Business Machines  
Corporation.

Java-related marks are trademarks or registered  
trademarks of Sun Microsystems Inc. in the  
United States and other countries.

Microsoft, Windows, Windows NT, and the  
Windows logo are trademarks of Microsoft  
Corporation in the United States, other  
countries, or both.

UNIX is a registered trademark of The Open  
Group in the United States and other countries.

Other trademarks and registered trademarks are  
the properties of their respective companies.

References in this publication to IBM products  
or services do not imply that IBM intends to  
make them available in every country in which  
IBM operates. Consult your local IBM business  
contact for information on the products,  
features, and services available in your area.

IBM hardware products are manufactured from  
new parts, or new and used parts. Regardless,  
our warranty terms apply.

Photographs shown are of engineering  
prototypes. Changes may be incorporated in  
production models.

This equipment is subject to all applicable FCC  
rules and will comply with them upon delivery.